Grant Thornton

The Escalation of Privacy

Preparing for NIST revisions

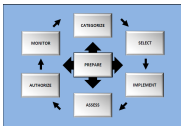
May 23, 2018

Discussion Topics

- Key enhancements and changes expected in the following NIST frameworks:

Security and Privacy Controls for Systems and Organizations (SP 800-53, rev 5) ***Target December 2018***

ID	FAMILY	ID	FAMILY
AC	Access Control	MP	Media Protection
AT	Awareness and Training	PA	Privacy Authorization
AU	Audit and Accountability	PE	Physical and Environmental Protection
CA	Assessment, Authorization, and Monitoring	PL	Planning
CM	Configuration Management	PM	Program Management
CP	Contingency Planning	PS	Personnel Security
IA	Identification and Authentication	RA	Risk Assessment
IP	Individual Participation	SA	System and Services Acquisition
IR	Incident Response	SC	System and Communications Protection
MA	Maintenance	SI	System and Information Integrity

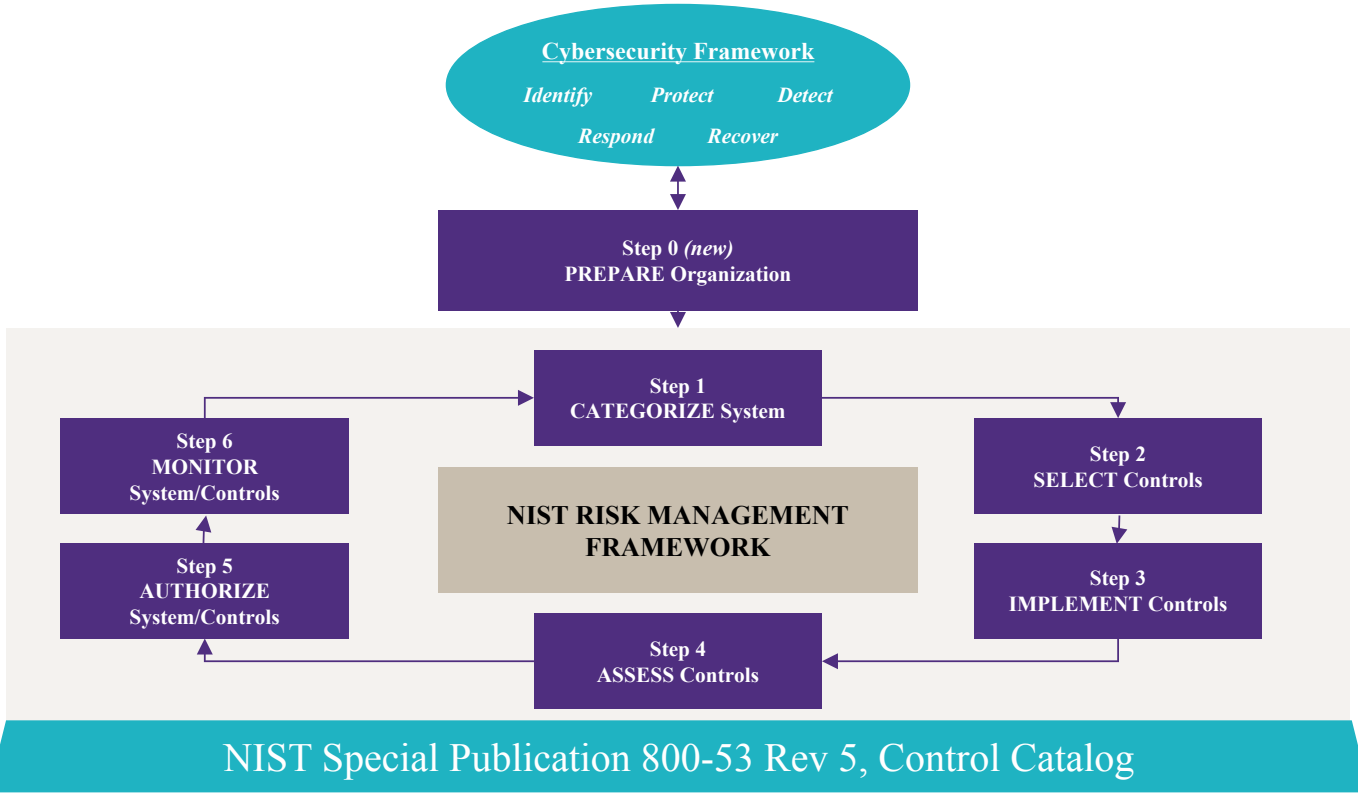


Guide for Applying the Risk Management Framework to Information Systems (SP 800-37, rev 2) – ***Target October 2018***

Cyber Security Framework (CSF version 1.1) – ***Final April 16, 2018***

- Interrelationship and complement of all three frameworks
- Preparation and Action

Integrated Framework for Privacy & Security

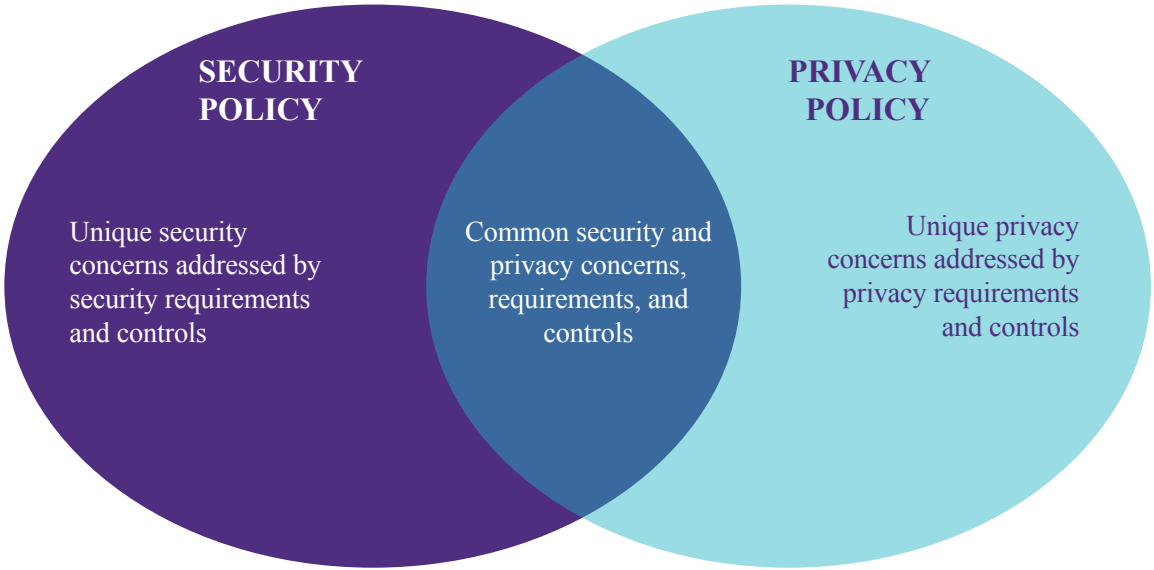


NIST Special Publication 800-53 Rev 5, Control Catalog

Key updates: NIST 800 53 Rev 5

- Security and Privacy Controls for Federal Information Systems and Organizations
- Expanded focus on cloud, mobile, cyber-physical, industrial/ process control systems, and IoT devices
- Outcome-based controls structure
- **Full integration of privacy controls into the security control catalog**
- Integration with the Cybersecurity Framework
- New controls based on threat intelligence and empirical attack data

NIST SP 800 53 Rev 5 – Privacy control integration



Confidentiality, Integrity, Availability

Information lifecycle: collect, use, store, transmit, dispose

NIST SP 800 53 Rev 5 – Privacy control integration

Two new required privacy control families reinforce Fair Information Practices Principles: Authority and Purpose, Use Limitation, Minimization, Notice, Choice, Access and Amendment

Individual Participation: Policies, procedures and controls regarding consent, redress, access, privacy notices, Privacy Act statements

Privacy Authorization: Comprehensive privacy program for authority to collect, purpose specification, and information sharing with external parties

ID	FAMILY	ID	FAMILY
AC	Access Control	MP	Media Protection
AT	Awareness and Training	PA	Privacy Authorization
AU	Audit and Accountability	PE	Physical and Environmental Protection
CA	Assessment, Authorization, and Monitoring	PL	Planning
CM	Configuration Management	PM	Program Management
CP	Contingency Planning	PS	Personnel Security
IA	Identification and Authentication	RA	Risk Assessment
IP	Individual Participation	SA	System and Services Acquisition
IR	Incident Response	SC	System and Communications Protection
MA	Maintenance	SI	System and Information Integrity

NIST SP 800 53 Rev 5 – Privacy control integration

TABLE E-2: AWARENESS AND TRAINING FAMILY

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	WITHDRAWN	PRIVACY-RELATED	IMPLEMENTED BY	ASSURANCE	CONTROL BASELINES		
						LOW	MOD	HIGH
AT-1	Awareness and Training Policy and Procedures		P	O	A	X	X	X
AT-2	Awareness Training		P	O	A	X	X	X
AT-2(1)	PRACTICAL EXERCISES		P	O	A			
AT-2(2)	INSIDER THREAT			O	A		X	X
AT-2(3)	SOCIAL ENGINEERING AND MINING			O	A		X	X
AT-3	Role-Based Training		P	O	A	X	X	X
AT-3(1)	ENVIRONMENTAL CONTROLS			O	A			
AT-3(2)	PHYSICAL SECURITY CONTROLS			O	A			
AT-3(3)	PRACTICAL EXERCISES		P	O	A			
AT-3(4)	SUSPICIOUS COMMUNICATIONS AND ANOMALOUS SYSTEM BEHAVIOR			O	A			

NIST SP 800 53 Rev 5 – Privacy control integration

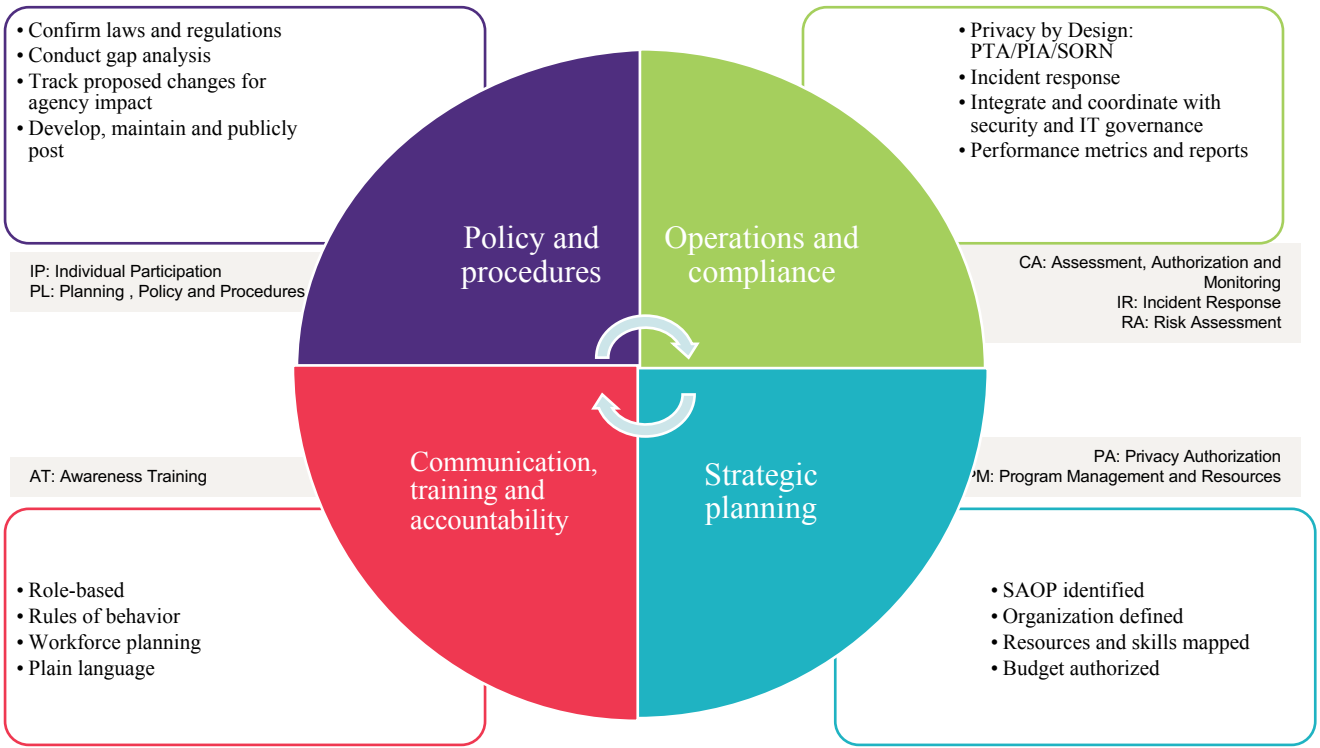
Appendix F (excerpt) –privacy-related control selection criteria

IP-1	Individual Participation Policies and Procedures	P	R
IP-2	Consent	P	S
IP-2(1)	Consent | ATTRIBUTE MANAGEMENT	P	D
IP-2(2)	Consent | JUST-IN-TIME NOTICE OF CONSENT	P	D
IP-3	Redress	P	S
IP-3(1)	Redress | NOTICE OF CORRECTION OR AMENDMENT	P	S
IP-3(2)	Redress | APPEAL	P	S
IP-4	Privacy Notice	P	S
IP-4(1)	Privacy Notice | JUST-IN-TIME NOTICE OF PRIVACY AUTHORIZATION	P	D

Ownership
Privacy Program (P) or Joint (J)

Selection Criteria
Required (R) : base on legal, regulatory or policy regs
Situationally Required (S): laws and regs that only apply in specific circumstances
Discretionary (D): optional based on privacy risk

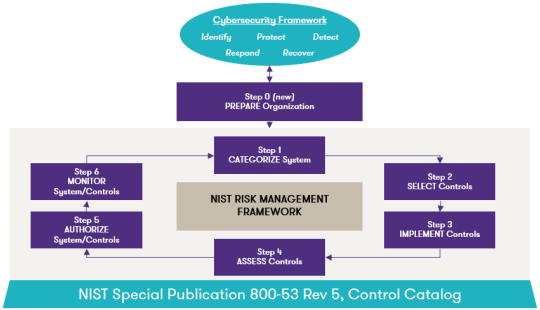
Privacy Authorization covers framework for total privacy management



Risk Management Framework - SP 800 37 Rev 2
Step 0 – Prepare the Organization

Expands business consideration and impact to not take time and getting commitment

- Identify missions, business functions, and processes that will be supported by the system
- Define organizational risk management strategy
- Identify stakeholders
- Conduct initial risk assessment and determine the value of organizational assets
- Define stakeholder protection needs and security requirements
- Determine system boundaries
- Identify how the system integrates into the enterprise and security architecture of the organization
- Identify and assign specific roles associated with RMF execution



Holistic approach tightens linkage and alignment to business mission

Prepare for new standards

- Engage Privacy Office
  - Create or refresh policy, procedures, narratives, etc.
  - Conduct training on NIST guidelines
  - Collaborate to identify and select privacy controls
- Update System Security Plans and other related documentation
- Review and integrate RMF rev 2, Step 0 tasks
  - New systems: Initiation
  - Legacy systems: Operations/maintenance
- Continue to integrate the frameworks across the enterprise

The escalation of privacy

Barbra Symonds, Director
barbra.symonds@us.gt.com
703 837 4534

Grant Thornton